REMARKS/ARGUMENTS

Claims 11-30 were pending in the application. Claims 29 and 30 have been withdrawn Claims 31- 42 are new and read onto the elected invention.

Election

Applicants confirm electing claims 11-28 for examination.

Rejection under 35 U.S.C. 112, second paragraph

Applicants respectfully disagree that claim 28 is indefinite. It is submitted that the examiner has not shown of the mistaken use of the article "the" in the first instance of "management computer." It is therefore traversed. It is obviously being made as a matter of custom, without any consideration of whether it in fact renders the claim indefinite. A simple request of correction would have been appropriate. Applicant has amended claim 28 to correct the mistake and conform to standard practice.

Amendments

The amendments to claim 11 are intended to remove a unnecessary limitation and to conform the claim to the account for the removed limitation. The amendments are neither narrowing nor being made in response to a rejection. Amendments to claims 11, 14, 15, 18, 19 and 20 are being made for formal reasons to remove "steps of" language. Although the examiner is not interpreting any limations of these claims as "steps for" elements pursuant to Section 112, paragraph 6, the amendments are being made to clarify that they should not be interpreted as "steps for" elements.

Rejection of as obvious under 35 U.S.C.103

The rejections of all pending claims under Section 103 are respectfully traversed.

The claimed subject matter relates to recovering an authorization code that is stored on an access-protected device – *e.g.* a "dongle" – when the authorization code on that device requires

restoration. The access-protected data processing device, when it is connected to a computer, authorizes use or access to, for example, an application on the computer. The application reads the code from the access-protected data processing device.

The apparatus and methods described in the primary reference, US2003/0074569 of Yamauchi et al. ("Yamauchi"), comprise backing up an encryption key – the "content key" – stored on a computer to a memory card. See paras. 0004-0005. The passages cited by the examiner from Yamauchi, namely paragraphs 0019 and 0030, appear to describe the recovery of a back-up copy of the content key from a memory card. The content key is stored in an encrypted form on the memory card. When the memory card is inserted into the content reproduction device, the content key is decrypted and copied onto the audio content reproduction device.

As understood by applicants, the examiner contends that all the limitations of independent claims 11 and 21 are essentially met by paragraph 0030 of Yamauchi, except for the limitations that a "security file" stores licensing parameters and the licensing parameters are sent to licensor. However, he asserts that a "security file" is taught by US2005/0144019 of Murakami et al. ("Murakami"), and that Murakami also teaches a licensor server in communication with a customer, where the server stores licensing information. The examiner then argues then that it would have been obvious to store the license parameters in a security file and to substitute a licensor server for the memory card used by Yamauchi, as the memory card and the licensor server each perform the same functions and the results would have been predictable.

Applicants respectfully disagree and submit that the examiner's reasoning for supporting rejections contains a number of errors, the most fundamental of which are identified below.

The processes of independent claims 11 and 21 relate to methods that involve recovering an authorization code from a licensor, not from the computer to which an "access-protected device" is connected. The methods use the licensee's computer to send to the licensor parameters stored on the licensee's computer, and then to receive back from the licensor an authorization code, which code is then stored on an access-protected device. These methods allow, if desired, the licensor to restore the original authorization code, or to rebuild or

regenerate a new authorization code, based on the sent parameters. For example, as mentioned in paragraph 0007 of the specification, licenses may be restricted in time or in use, or can be so-called pay-per-use licenses. Having parameters for the license stored in a file allows, in the case of these type of licenses, the last state of the license, before the authorization code became unavailable, to be stored and made available for use by the licensor in restoring the authorization code. The methods are thus suitable for use not only with stateless security systems, but also stateful security systems.

Although there are a number of errors in the reasoning underlying rejections of the independent claims, as well as each of the dependent claims, applicants would like to address the most notable errors, reserving for later the opportunity to address the remaining errors.

First, the apparatus-specific ID, which the examiner is apparently contending is a license parameter, does not appear to be a license parameter. Rather, the apparatus-specific ID is being used solely to ensure that memory card transmits the content key only to the content reproduction device from which the content key was received. In other words, it appears to be just a copy prevention scheme. Yamauchi explains in paragraph 0009:

> To prepare for a possible breakdown of the hard disk in such a content reproduction apparatus, it is advisable to back up the content; however, the content body can not be readily backed up due to its great data size. Because the user can obtain the content body free at any time, the content body need not be backed up. Thus, it is only necessary to back up the content key data for decrypting the content; however, in case the backed-up content key data is allowed to be unfairly used by any other apparatus than the user's content reproduction apparatus, it is very likely that the copyright of the content will not be appropriately protected. Therefore, according to the present invention, an apparatus-specific code is imparted to the content reproduction apparatus of the user, and, when the backed-up content key data is to be restored from the backup storage medium to a particular content reproduction apparatus, a comparison is made between the apparatus-specific code written in the backup storage medium along with the content key data and an apparatus-specific code imparted to the particular content reproduction apparatus. (emphasis supplied)

Given that Yamauchi identifies the possibility that other devices can use the content key as the concern being addressed by the invention, applicants submit that the content key is not

issued to a specific apparatus and, therefore, the apparatus-specific ID of Yamauchi cannot be a parameter of the license. It is a parameter only of the apparatus.

Second, the process set forth in paragraph 0030 does not in fact meet, as the examiner appears to contend, the limitation of "storing the restored authorization code in the data-processing device connected to the computer of the licensee in a device-specific format in the data-processing device." This process step occurs after the authorization code – the "restored authorization code" -- is returned from the licensor, which occurs after the license parameters are sent.

The content reproduction device of Yamauchi is the device to which the content key is to be restored. Thus, it would have to correspond to the "data processing device" in the claims for the process of Yamauchi to meet the limitations in the manner contended by the examiner. In Yamauchi, the apparatus specific ID is transmitted by the content reproduction device to the memory card, which then compares it to the apparatus specific ID it has stored for the content key that it also stored. If they match, the memory card then transmits the content key back to the content reproduction device, thus restoring it.

The claim requires that an authorization code be stored in a device-specific format in the data processor device. The examiner cites Fig. 2 of Yamauchi and the text describing it as meeting this limitation, but, Fig. 2 illustrates the configuration of the memory card. The memory card has already stored the content key described. There is no indication in Yamauchi that applicants can find specifying how the content key is stored in its content reproduction device, let alone in a device-specific format.

Third, it submitted that the combination of Yamauchi and Murakami fails short of the meeting the limitations of claims 11 and 21. As already mentioned, the examiner argues that it would have been "obvious … to use the licensor server of Murakami in place of the memory card of Yamauchi to back up the license key…." Claims 11 and 21 require that a licensee's computer read the license parameters from its memory, to send them to a licensor. If a licensor server is substituted for the memory card in the process of claim 0030, the combination fails to teach an "access protected data processing device" connected to they licensee's computer, as

required by claims 11 and 21, to which the restored authorization code is saved once it is returned from the licensor.

Given that substantial errors underlie each ground of rejection, it is submitted that no prima facie rejection of any of the claims has been established and that, in fact, that the pending claims are allowable over the art of record for at least the foregoing reasons. Applicants therefore see no need to address the remaining errors, especially as to the dependent claims. By not addressing the remaining errors or any particular interpretation given to the claims or to the prior art, applicants do not intend to waive the right to complain of the errors or to exhibit acquiescence to any particular interpretation.

New Claims

New claims 31 and 33, which depend from claims 11 and 21, respectively, specify that the security file on the licensee's computer storing the license parameters does not store the authorization code. New claim 32 specifies that the authorization code cannot be stored anywhere but on the access-protected data processing device. It is submitted that these claims are allowable over the art of record for at least these reasons.

New claims 34-42 define a computer readable medium for storing computer instructions for performing a process for restoring an authorization code. Claim 34 is allowable over the art of record for at least the same reasons as claim 11.

In conclusion, it is submitted that the claims are allowable for the reasons set forth above. Allowance of the application is respectfully requested.

Applicants hereby authorize the Commissioner to charge any fees due but not submitted with this paper to Deposit Account No. 07-0153. The Examiner is respectfully requested to call Applicants' Attorney for any reasons that would advance the current application to issue. Please reference Attorney Docket No. 125542-1006.

Respectfully submitted,

GARDERE WYNNE SEWELL LLP

/Marc A. Hubbard/

Marc A. Hubbard
Registration No. 32,506
ATTORNEY FOR APPLICANT

Date: November 26, 2008

3000 Thanksgiving Tower
1601 Elm Street
Dallas, Texas 75201-4761
(214) 999-4880 - Telephone
(214) 999-3880 - Facsimile

DALLAS 1993239v.1